



DEPARTMENT OF HOMELAND SECURITY

6 CFR Chapter I

49 CFR Chapter XII

Ratification of Security Directives

AGENCY: Office of Strategy, Policy, and Plans, Department of Homeland Security (DHS).

ACTION: Notification of ratification of security directives.

SUMMARY: DHS is publishing official notice that the Transportation Security Oversight Board (TSOB) has ratified Transportation Security Administration (TSA) Security Directive 1580-21-01, Security Directive 1582-21-01, Security Directive Pipeline-2021-01A, and Security Directive Pipeline-2021-02B. Security Directive 1580-21-01 requires owners/operators of specified freight railroad carriers to implement certain measures addressing cybersecurity vulnerabilities. Security Directive 1582-21-01 applies these same requirements to owner/operators of specified passenger railroad carriers and rail transit systems. Security Directive Pipeline-2021-01A and Security Directive Pipeline-2021-02B amend earlier cybersecurity directives applicable to owner/operators of critical pipeline systems and facilities. Security Directive Pipeline-2021-01A incorporates a revised definition of a “cybersecurity incident” and aligns the definition with the definition applicable across other modes of transportation regulated by TSA. Security Directive Pipeline-2021-02B provides additional flexibility to owner/operators in complying with the mitigation measures required by Security Directive Pipeline-2021-02.

DATES: The TSOB ratified Security Directive 1580-21-01, Security Directive 1582-21-01, and Security Directive Pipeline-2021-01A on December 29, 2021. The TSOB ratified Security Directive Pipeline-2021-02B on January 13, 2022.

FOR FURTHER INFORMATION CONTACT: Thomas McDermott, Acting Assistant Secretary for Cyber, Infrastructure, Risk and Resilience Policy at 202-834-5803 or thomas.mcdermott@hq.dhs.gov.

SUPPLEMENTARY INFORMATION:

I. Background

A. Cybersecurity Threat

Cybersecurity incidents affecting surface transportation entities are a growing threat that pose a risk to the national and economic security of the United States. In recent years, cyber attackers have maliciously targeted the critical infrastructure of surface transportation modes in the United States, including pipelines, freight railroads, passenger railroads, and rail transit systems, with multiple cyberattack and cyber espionage campaigns.¹ This threat continues to evolve and is ongoing. By targeting the integrated cyber and physical infrastructure of surface transportation entities, these attackers threaten the safe, secure, and uninterrupted daily operation of surface transportation systems relied upon by the U.S. economy with potential to cause nationwide impact.

B. Security Directive 1580-21-01 and Security Directive 1582-21-01

In response to this persistent threat, TSA issued two security directives on December 2, 2021, requiring specified surface transportation entities to implement urgently needed measures that immediately enhance the cybersecurity of the surface

¹ These activities include the April 2021 breach of New York City's Metropolitan Transportation Authority (the nation's largest mass transit agency) by hackers suspected to be linked to the Chinese government; the December 2020 "Sunburst" attack on transit agencies; the August 2020 attack on the Southeastern Pennsylvania Transportation Authority; the 2017 ransomware attack on the Sacramento Regional Transit District; and the November 2016 ransomware attack on the San Francisco Municipal Transportation agency. This threat is ongoing: for example, on November 17, 2021, the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre, and the United Kingdom's National Cyber Security Centre issued a joint cybersecurity advisory highlighting ongoing malicious cyber activity by an advanced persistent threat group (APT) that these agencies associated with the government of Iran. The advisory states that "The Iranian government-sponsored APT actors are actively targeting a broad range of victims across multiple U.S. critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector, as well as Australian organizations." Alert AA21-321A (November 17, 2021).

transportation sector.² Specifically, the two materially identical security directives—one applicable to specified freight railroad carriers and the other applicable to specified passenger railroad carriers and rail transit systems—require owner/operators to take the following four crucial actions:

- Designate a Cybersecurity Coordinator who is required to be available to TSA and CISA at all times (all hours/all days) to coordinate implementation of cybersecurity practices, manage cybersecurity incidents, and serve as a principal point of contact with TSA and CISA for cybersecurity-related matters;
- Report cybersecurity incidents to CISA;
- Conduct a Cybersecurity Vulnerability Assessment to identify gaps in current cybersecurity measures, identify remediation measures, and develop a plan for the owner/operator to implement the remediation measures to address any identified vulnerabilities and gaps; and
- Develop a Cybersecurity Incident Response Plan to reduce the risk of operational disruption should their Information and/or Operational Technology systems be affected by a cybersecurity incident.

The actions required by these security directives only apply to specified owner/operators of freight railroads, passenger railroads, and rail transit systems that TSA has determined are higher risk.³ The covered entities are those that the nation depends on to move passengers and transport freight in support of critical sectors, including national defense.

² 49 U.S.C. 114(l)(2)(A).

³ See 49 CFR 1580.101 and 1582.101. On December 2, 2021, TSA separately issued an Information Circular (IC) to TSA-regulated owner/operators of freight railroads, passenger railroads, public transportation agencies, and rail transit systems not specifically covered by the security directives and -over-the-road-bus owner/operators regulated under 49 CFR part 1584, recommending that these entities generally implement the same four actions that the security directives require of higher-risk surface transportation entities. See Surface Transportation Information Circular-2021-01.

Both security directives became effective on December 31, 2021 and are set to expire on December 31, 2022.⁴

C. TSA Security Directive Pipeline-2021-01A

On December 2, 2021, TSA also issued a security directive amending a directive issued earlier that year requiring owner/operators of critical pipeline systems and facilities to implement certain cybersecurity measures. On May 26, 2021, TSA issued Security Directive Pipeline-2021-01, which was the first of multiple security directives issued by TSA in 2021 to enhance the cybersecurity of critical pipeline systems in response to the ransomware attack on the Colonial Pipeline Company on May 8, 2021. This first directive required owner/operators to: (1) report cybersecurity incidents to CISA; (2) appoint a cybersecurity coordinator to be available 24/7 to coordinate with TSA and CISA; and (3) conduct a self-assessment of cybersecurity practices, identify any gaps, and develop a plan and timeline for remediation.⁵ This security directive went into effect on May 28, 2021, and was ratified by the TSOB on July 3, 2021. 86 FR 38209. It is set to expire on May 28, 2022.

Security Directive Pipeline-2021-01A, issued on December 2, 2021, amended Security Directive Pipeline-2021-01, updating the definition of cybersecurity incident applicable in the pipeline context to mirror the definition used by the subsequent security directives applicable to specified surface transportation sector entities. TSA's determination to use a modified definition was made following industry input and consultation with DHS cybersecurity experts. The amended definition of cybersecurity incident applicable to critical pipeline owner/operators provides further clarity regarding the nature of incidents that fall within the definition of cybersecurity incident and ensures

⁴ TSA's security directives are presumptively Sensitive Security Information (SSI) by regulation and are subject to disclosure restrictions. 49 CFR 1520.5(b)(2). The TSA Administrator, however, has determined that it is in the interest of public safety and in furtherance of transportation security that Security Directive 1580-21-01 and Security Directive 1582-21-01 be made publicly available. 49 CFR 1520.5(b).

⁵ 86 FR 38209.

the consistent identification of incidents that must be reported to CISA across all covered modes of transportation.

D. TSA Security Directive Pipeline-2021-02B

On July 19, 2021 TSA issued the second security directive—Security Directive Pipeline-2021-02—in response to the Colonial Pipeline attack, building on the requirements of Security Directive Pipeline-2021-01 to further enhance the cybersecurity of critical pipeline systems. Security Directive Pipeline-2021-02 required owner/operators of critical pipelines to take the following additional actions:

- Implement specified mitigation measures to reduce the risk of compromise from a cyberattack;
- Develop a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption or functional degradation of information technology and operational technology systems in the event of a malicious cyber intrusion; and
- Test the effectiveness of their cybersecurity practices through an annual cybersecurity architecture design review conducted by a third party.

Security Directive Pipeline-2021-02 became effective on July 26, 2021 and was ratified by the TSOB on August 17, 2021. 86 FR 52953 (September 24, 2021). It is set to expire on July 26, 2022.

On December 17, 2021, TSA issued Security Directive Pipeline-2021-02B, amending Security Directive Pipeline-2021-02 to provide additional flexibility to owner/operators in complying with the directive's requirements. TSA amended the directive's requirements based on industry feedback and following consultation with CISA. The revisions provide pipeline owner/operators with the necessary flexibility to

comply with the directive's requirements, while ensuring that the requirements are met in a uniform and operationally safe manner.⁶

II. TSOB Ratification

TSA has broad statutory responsibility and authority to safeguard the nation's transportation system.⁷ The TSOB—a body consisting of the Secretary of Homeland Security, the Secretary of Transportation, the Attorney General, the Secretary of Defense, the Secretary of the Treasury, the Director of National Intelligence, or their designees, and a representative of the National Security Council—reviews certain TSA regulations and security directives consistent with law.⁸ TSA issued each of these security directives under 49 U.S.C. 114(l)(2)(A), which authorizes TSA to issue emergency regulations or security directives without providing notice or public comment where “the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security”. Security directives issued pursuant to the procedures in 49 U.S.C. 114(l)(2) “shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Board or rescinded by the Administrator.”⁹

Following the issuance of Security Directive 1580-21-01, Security Directive 1582-21-01, and Security Directive Pipeline-2021-01A on December 2, 2021, the chairman of the TSOB convened the board for the purpose of reviewing each directive. Following the issuance of Security Directive Pipeline-2021-02B on December 17, 2021, the chairman again convened the board for the purpose of reviewing that directive. In reviewing the directives, the TSOB reviewed the actions required by Security Directive

⁶Security Directive Pipeline-2021-02B and its specific requirements for operators are designated as Sensitive Security Information (SSI) under TSA regulations. *See* 49 CFR 1520.5(b)(1), (b)(2), (b)(6), (b)(8). Absent a determination by the TSA Administrator to remove the SSI designation in the interest of public safety or in furtherance of transportation security, Security Directive Pipeline 2021-02B, the records produced in compliance with its requirements, and the information contained in these records remain designated as SSI and afforded the protections of such a designation. *See* 49 CFR 1520.5(b).

⁷ *See, e.g.*, 49 U.S.C. 114(d), (f), (l), (m).

⁸ *See, e.g.*, 49 U.S.C. 115; 49 U.S.C. 114(l)(2)(B).

⁹ 49 U.S.C. 114(l)(2)(B).

1580-21-01 and Security Directive 1582-21-01 to mitigate cybersecurity vulnerabilities in the rail transportation sector; the need for TSA to issue the security directives pursuant to its emergency authority under 49 U.S.C. § 114(l)(2) to prevent the disruption and degradation of the country's critical rail transportation infrastructure; Security Directive Pipeline-2021-01A's amended definition of cybersecurity incident applicable to owner/operators of critical pipeline systems and facilities; and the flexibilities provided by Security Directive Pipeline-2021-02B. Following its review, the TSOB ratified all four security directives. The TSOB ratified Security Directive 1580-21-01, Security Directive 1582-21-01, and Security Directive Pipeline-2021-01A on December 29, 2021. The TSOB ratified Security Directive Pipeline-2021-02B on January 13, 2022.

John K. Tien

Deputy Secretary of Homeland Security & Chairman of the Transportation Security Oversight Board.

[FR Doc. 2022-11018 Filed: 5/20/2022 8:45 am; Publication Date: 5/23/2022]